	Application No.	Applicant(s)	
Notice of Allowability	10/518,605	GERTNER, DMITRY ALEXANDROVICH	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *interview on 6/27/2007*.

2. ☒ The allowed claim(s) is/are *56-72*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☒ All   b) ☐ Some*   c) ☐ None   of the:

        1. ☒ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of
    Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *6/27/2007* .

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

CHRISTOPHER REVAK
PRIMARY EXAMINER

DETAILED ACTION

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's Amendment was given in a telephone interview with Judson K. Champlin (Reg. No. 34,797) on 27 June 2007.

This application has been amended as follows:

IN THE CLAIMS

Cancel claim 1 – 55 and 73 – 74.

Replace claims 56 and 68.

Claim 56:

A method for transmission of information with protection against copying with use of a personal cryptoprotective complex designed for both transmission and reception of information, the method comprising:

in a ROM of each of personal cryptoprotective complexes, storing a mother code

being a set of random numbers (M1, M2, ..., MN), copies of encryption, decryption and

information processing programs, wherein record is carried out in a protected way only

in said personal cryptoprotective complexes, said way excluding the possibility of

recording to other media and modifying said programs, as well as personal data of a

user including his or her electronic signature, and setting date and time in a built-in

clock;

generating and storing an electronic document in a PROM of the personal

cryptoprotective complex;

establishing a protected communication session with application of the personal

cryptoprotective complexes on the basis of a single-use key of the communication

session generated using random numbers and the mother code, and inputting a user's

command to transmit the electronic document recorded in the PROM to other

subscriber of the established communication session;

encrypting the electronic document by <u>a dynamically transformable daughter</u>

<u>code on the basis of the mother code and the single-use encryption key in the personal</u>

<u>cryptoprotective complexes of users</u> an encryption program and transmitting the

encrypted electronic document to another personal cryptoprotective complex;

upon termination of transmission of the encrypted electronic document, in the

personal cryptoprotective complex, disabling any operations with the electronic

document stored in the PROM for a predetermined time period T1;

in the personal cryptoprotective complex of a receiving party, receiving the

encrypted electronic document, performing decryption by a decryption program, and

obtaining the electronic document;

recording the electronic document to the PROM, and disabling any operations

with the electronic document for a predetermined time period T1;

generating an electronic-document-loading-acknowledgement password in the

personal cryptoprotective complex of a receiving party and transmitting the electronic-

document-loading-acknowledgement password in the encrypted form to the personal

cryptoprotective complex of a sending party;

in case if the sender does not receive the electronic-document-loading-

acknowledgement password from the recipient during the time period T1, enabling the

electronic document in the PROM of the personal cryptoprotective complex of the

sender, while ignoring the subsequent reception of said password;

in case if the recipient does not send the electronic-document-loading-

acknowledgement password to the sender during the time period T1, automatically

deleting the electronic document from the PROM of the personal cryptoprotective

complex;

receiving the electronic-document-loading-acknowledgement password in the

personal cryptoprotective complex of the sending party, generating an electronic-

document-transmission-acknowledgement password, and requesting a user acknowledgement in response to the sending of the present password to the personal cryptoprotective complex of the receiving party;

in case if the user gives no acknowledge in response to the sending of the password during a predetermined time period T2, then, on the expiration of said time period, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender, and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user acknowledges the sending of the password during the time period T2, sending the present password in the encrypted form to the personal cryptoprotective complex of the recipient, wherein said electronic document is automatically deleted from PROM of the personal cryptoprotective complex of the sender, and said electronic document is automatically enabled in the PROM of the personal cryptoprotective complex of the recipient when he or she has received said electronic-document-transmission-acknowledgement password, and is outputted to the user.

Claim 68:

A method for simultaneously exchanging copy-protected electronic documents among users through a communication link with use of a cryptoprotective complex designed for both transmission and reception of information, comprising:

in a ROM of each of personal cryptoprotective complexes, storing a mother code

being a set of random numbers (M1, M2, ..., MN), encryption, decryption and

information processing programs, wherein record is carried out in a protected way only

in said personal cryptoprotective complexes, said way excluding the possibility of

recording to other media and modifying said programs;

storing an individual number I of the personal cryptoprotective complex in the

ROM as well as personal data of a user including his or her electronic signature, and

setting date and time in a built-in clock;

synchronously generating a single-use encryption key on the basis of random

numbers produced in the personal cryptoprotective complexes of users and the mother

code;

synchronously generating dynamically transformable daughter codes on the

basis of the mother code and the single-use encryption key in the personal

cryptoprotective complexes of users and encrypting the electronic document by the

daughter code and transmitting the encrypted electronic document to another personal

cryptoprotective complex;

inputting initial information to each of the personal cryptoprotective complexes of

users and storing the obtained electronic document in the PROM of the personal

cryptoprotective complex;

in at least one of the personal cryptoprotective complexes, inputting a command

for simultaneous exchanging the electronic documents, and sending said command in

the form of a signal encrypted by means of the produced single-use encryption key to other personal cryptoprotective complex;

in each of the personal cryptoprotective complexes, inputting a user's command to start transmission of the electronic document recorded in the PROM to other subscriber of the established communication session;

encrypting the electronic document by an encryption program, and transmitting the encrypted electronic document to other personal cryptoprotective complex;

in accordance with the command for simultaneous exchanging the electronic documents, disabling any operations with the electronic document stored in the PROM for a predetermined time period T1;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortions in information by a decryption program, recording the electronic document to the PROM, disabling any operations with the electronic document for a predetermined time period T1, and outputting the obtained electronic document to the user for acquaintance;

in the personal cryptoprotective complex of the receiving party, generating an electronic-document-loading-acknowledgement password and transmitting said electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of the sending party;

in case if the sender does not receive the electronic-document-loading-acknowledgement password from the recipient during the time period T1, the electronic

document is enabled in the PROM of the personal cryptoprotective complex of the sender;

in case if the recipient does not send the electronic-document-loading-acknowledgement password to the sender during the time period T1, automatically deleting the electronic document from the PROM of the personal cryptoprotective complex of the recipient;

receiving the electronic-document-loading-acknowledgement in the personal cryptoprotective complex of sending party, generating an electronic-document-transmission-acknowledgement password and requesting a user acknowledgement to send the present password to the personal cryptoprotective complex of the receiving party;

in case if the user does not acknowledge the sending of the password during a predetermined time period T2, then, after the expiration of said time period, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender, and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user gives the acknowledgement for sending the password during the time period T2, then, sending a predetermined signal in the encrypted form containing information of said acknowledgement to other user, and receiving a similar signal from said user;

after the exchange of acknowledgement signals, making synchronization according the last signal, and from the moment of sending a last bit of said signal from

one of personal cryptoprotective complexes and, respectively, the moment of reception thereof in other personal cryptoprotective complex, starting a procedure of a simultaneous exchange of the electronic-document-transmission-acknowledgement passwords in the encrypted form, wherein the reception of a password-containing signal from the opposite party is monitored in each of the personal cryptoprotective complexes, and in case of absence or interruption of said signal, the transmission of own password is stopped;

after the sending of the transmission-acknowledgement password, automatically deleting said electronic document from the PROM of the personal cryptoprotective complex of the sender, and when the recipient has received the electronic-document-transmission-acknowledgement password, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the recipient.

Allowable Subject Matter

Claims 56 – 72 are allowed.

The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claims 56, 62 and 68.

The prior arts fail to teach or suggest a method for transmission of information with protection against copying with use of a personal cryptoprotective complex by

receiving the electronic-document-loading-acknowledgement password in the personal

cryptoprotective complex of the sending party from the recipient within the first time

period T1, generating an electronic-document-transmission-acknowledgement

password from the sender; in case if the user acknowledges the sending of the

password during the second time period T2, sending the present password in the

encrypted form to the recipient, wherein said electronic document is automatically

deleted from PROM of the the sender, and said electronic document is automatically

enabled in the PROM of the recipient when said electronic-document-transmission-

acknowledgement password has been received, followed by inputting user's

commands, processing the decrypted information according to the user's commands

received from the service information and according to the earlier inputted information

and the information processing program, and outputting the processed information to

the user together with service symbols that authenticate attributes of the received

electronic document. The closest prior art, U.S. Pattern 7,093,015 and U.S. Pattern

5,671,279, fails to anticipate or render obvious the claimed invention.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Longbit Chai whose telephone number is 571-272-3788.

The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

CHRISTOPHER REVAK
PRIMARY EXAMINER